УТВЕРЖДЕНА
Приказом и.о. директора
МАУ ДО ЦДТ «Исток» г. Перми
от 23.11.2017 г. N 62

ПОЛИТИКА
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МАУ ДО ЦДТ «Исток» г. ПЕРМИ

I. Общие положения

1.1. Настоящая Политика информационной безопасности МАУДО ЦДТ «Исток» г.Перми (далее - Политика ИБ) разработана в целях установления безопасных способов обработки информации в электронном виде, в том числе в информационных системах (сайтах) (далее - информационная система) МАУДО ЦДТ «Исток» г.Перми (далее ЦДТ).

1.2. Настоящая Политика ИБ определяет цели и задачи защиты информации, устанавливает методы защиты информации, которыми должны руководствоваться сотрудники ЦДТ, при обработке информации в электронном виде, в том числе в информационных системах, ответственность сотрудников за нарушение требований настоящей Политики ИБ.

1.3. Настоящая Политика ИБ применима ко всем техническим средствам (серверам, периферийному оборудованию, автоматизированным рабочим местам (далее - АРМ) и так далее), ко всем процессам обработки информации с использованием указанных технических средств.

1.4. Правовыми основаниями настоящей Политики ИБ являются Конституция Российской Федерации, Гражданский кодекс Российской Федерации, Уголовный кодекс Российской Федерации, Кодекс Российской Федерации об административных правонарушениях, Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации", иные нормативные правовые акты Российской Федерации, документы Федеральной службы по техническому и экспортному контролю, Федеральной службы безопасности, Федеральной службы по надзору в сфере связи и массовых коммуникаций.

II. Термины и определения

В настоящей Политике ИБ используются следующие термины и определения:

вирус (компьютерный, программный) - исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения;

вредоносная программа - программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных;

доступность информации - состояние информации, при котором субъекты, имеющие санкционированные права доступа, могут реализовать их беспрепятственно;

защищаемая информация - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации;

идентификатор (имя, логин) - набор символов, представляющий уникальное наименование объекта или субъекта в информационной системе, позволяющее однозначно идентифицировать пользователя при входе его в систему, определить его права в ней, фиксировать действия и тому подобное;

информационная безопасность - состояние защищенности информационной среды;

информационная среда - совокупность условий для технологической переработки и эффективного использования информационных ресурсов (в том числе технические средства,

программное обеспечение, телекоммуникации, уровень подготовки пользователей, формы контроля, документопотоки, процедуры, регламенты, юридические нормы, иные факторы, воздействующие на информационные процессы и информационные системы);

информационные ресурсы - отдельные документы, массивы документов, в том числе содержащиеся в информационных системах (архивах, фондах, банках данных, других информационных системах);

инцидент информационной безопасности - любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность;

несанкционированное действие - действие субъекта в нарушение установленных в информационной системе регламентируемых правил обработки информации;

пароль - конфиденциальная последовательность символов, связанная с субъектом и известная только ему, позволяющая его аутентифицировать, то есть подтвердить соответствие реальной сущности субъекта предъявляемому им при входе идентификатору;

профиль - набор установок и конфигураций, специфичный для данного субъекта или объекта и определяющий его работу в информационной системе;

системный администратор - лицо, обеспечивающее выполнение функций по обеспечению работы компьютерной техники, сети и программного обеспечения

угроза безопасности информации - потенциально возможное событие, действие, процесс или явление, которое может привести к нарушению конфиденциальности, целостности, доступности информации, а также неправомерному тиражированию, которое наносит ущерб собственнику, владельцу или пользователю информации;

уязвимость - свойство информационной системы, обусловливающее возможность реализации угроз безопасности, обрабатываемой в ней информации;

целостность информации - состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими санкционированное право на изменение информации.

III. Цели и задачи защиты информации , основные виды угроз безопасности информации

3.1. Обеспечение информационной безопасности в ЦДТ (защита информации) - деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и (или) непреднамеренных воздействий на защищаемую информацию, ее носители, процессы обработки.

3.2. В ЦДТ обрабатывается информация различных уровней конфиденциальности:

общедоступная (открытая) информация, для которой требуется обеспечение доступности и целостности;

информация ограниченного распространения, доступ к которой ограничивается в соответствии с действующим законодательством Российской Федерации (далее - конфиденциальная информация), и наравне с доступностью и целостностью требуется обеспечение конфиденциальности.

Уровень конфиденциальности устанавливается обладателем информации.

3.3. Основными задачами защиты информации в ЦДТ являются:

выявление и оценка потенциальных угроз информационной безопасности и уязвимостей объектов защиты;

исключение либо минимизация выявленных угроз безопасности;

предотвращение инцидентов информационной безопасности.

3.5. Угрозы безопасности информации могут быть реализованы за счет:

утечки по техническим каналам утечки информации;

несанкционированного доступа с использованием соответствующего программного обеспечения.

3.6. Угрозы безопасности информации могут проявляться в виде инцидентов информационной безопасности:

утрата информации, оборудования или устройств;

системные сбои или перегрузки;

противоправные и (или) ошибочные действия служащих при работе на АРМ;

нарушение правил обработки информации, в том числе разглашение паролей доступа к информационным ресурсам, которые повлекли или могли повлечь нарушение конфиденциальности, целостности и (или) доступности информации;

нарушение физических мер защиты;

неконтролируемые изменения систем;

сбои программного обеспечения, отказы в обслуживании сервисов, средств обработки информации, оборудования;

нарушение правил доступа;

внедрение вредоносных программ.

3.7. В качестве методов защиты информации в ЦДТ применяются:

регламентация доступа в служебные помещения;

разграничение доступа к техническим средствам и информационным ресурсам;

применение антивирусной защиты;

применение криптографической защиты информации;

применение обезличивания персональных данных;

регламентация использования электронной почты;

регламентация работы в сети Интернет;

регламентация создания и эксплуатации информационных систем;

проведение внутреннего контроля и обучение сотрудников.

IV. Регламентация доступа в служебные помещения

4.1. Регламентация доступа в служебные помещения осуществляется в целях:

обеспечения физической сохранности носителей информации, оборудования;

исключения возможности несанкционированного доступа в служебные помещения, в том числе, в которых ведется обработка конфиденциальной информации.

4.2. Доступ сотрудников и посетителей в административные помещения осуществляется в соответствии с Положением о пропускном и внутриобъектовом режимах , утвержденным приказом директора ЦДТ.

V. Разграничение доступа к техническим средствам и информационным ресурсам

5.1. Разграничение доступа к техническим средствам и информационным ресурсам направлено на предотвращение получения информации, обрабатываемой в электронном виде, в том числе в информационных системах, с нарушением регламентируемых нормативными правовыми актами или владельцами информации правил, следствием которых может быть нарушение конфиденциальности, целостности и (или) доступности информации.

5.2. Для работы с информационными ресурсами сотруднику предоставляется АРМ.

ПО АРМ устанавливается и обновляется системным администратором со специальных ресурсов или съемных носителей в соответствии с лицензионным соглашением.

При передаче АРМ другому сотруднику производится удаление профиля пользователя АРМ.

5.3. Доступ к конфиденциальной информации, в том числе персональным данным, осуществляется в соответствии с установленным Положением об обработке и организации защиты персональных данных в ЦДТ.

5.4. К работе с информационными ресурсами ЦДТ допускаются сотрудники, ознакомленные с настоящей Политикой ИБ.

5.5. Для осуществления доступа к информационным ресурсам сотруднику создается учетная запись - присваивается уникальный идентификатор (имя, логин) и пароль доступа.

5.6. Для защиты своих паролей сотрудники обязаны:

соблюдать конфиденциальность пароля - не сообщать пароль другим лицам, в том числе другим сотрудникам, не хранить пароли в легкодоступных местах (на столе, стене, терминале и так далее);

выбирать трудно угадываемый пароль - использовать в пароле строчные и прописные буквы, цифры, специальные символы, не использовать в качестве пароля свои фамилию, имя, отчество, цифровые ряды или повторяющиеся цифры (123456, 111111 и так далее);

использовать в пароле не менее 8 символов;

в случае компрометации пароля немедленно изменить пароль.

5.7. При работе на АРМ сотрудники обязаны:

работать только под своей учетной записью;

блокировать доступ к АРМ при отсутствии на рабочем месте.

5.8. Сотрудникам запрещается самостоятельно устанавливать на АРМ дополнительные технические средства и (или) ПО.

VI. Антивирусная защита

6.1. Антивирусная защита применяется с целью защиты информационных ресурсов и ПО от несанкционированных действий (утраты, модификации, изменения) путем внедрения в информационную среду вирусов, вредоносных программ (далее - вирус) посредством использования специализированного ПО (далее - антивирусное ПО).

6.2. Антивирусное ПО должно быть развернуто на всех технических средствах, подверженных воздействию вирусов (АРМ, серверах). Антивирусные механизмы должны быть актуальными, постоянно включенными. Должны вестись журналы протоколирования событий. Отключение антивирусного ПО или отказ от автоматического обновления антивирусных баз не допускается.

6.3. При установке антивирусного ПО системным администратором должны выполняться

следующие требования:

актуализация антивирусных баз на АРМ, подключенных к локальной сети ЦДТ, должна осуществляться ежедневно в автоматическом режиме через специальный сервер обновлений;

актуализация антивирусных баз на АРМ, не подключенных к локальной сети ЦДТ, должна осуществляться с использованием съемных носителей информации не реже одного раза в неделю;

проверка критических областей АРМ, заражение которых вирусами может привести к серьезным последствиям, должна проводиться автоматически при каждой его загрузке.

6.4. Некоторые признаки проявления вируса:
прекращение работы или неправильная работа ранее успешно функционировавшего ПО;
медленная работа АРМ;
невозможность загрузки операционной системы;
нетипичная работа ПО;
вывод на экран непредусмотренных сообщений или изображений;
подача непредусмотренных звуковых сигналов;
частые зависания и сбои в работе АРМ;
частое появление сообщений о системных ошибках;
исчезновение файлов, каталогов или искажение их содержимого;
изменение даты и времени модификации файлов;
изменение размеров файлов;
неожиданное значительное увеличение количества файлов на диске;
существенное уменьшение размера свободной оперативной и дисковой памяти.

6.5. Для исключения заражения вирусами и обеспечения надежного хранения информации в электронном виде сотрудники обязаны:

убедиться, что на АРМ установлено и включено антивирусное ПО;

незамедлительно сообщить системному администратору о нарушениях работы антивирусного ПО;

перед использованием проверять съемные носители информации на наличие вирусов средствами установленного на АРМ антивирусного ПО;

при переносе на свой АРМ файлов в архивированном виде проверять их до и после разархивации на жестком диске, ограничивая область проверки только вновь записанными файлами;

использовать антивирусное ПО для входного контроля всех файлов (исполняемых файлов, файлов данных, сообщений электронной почты и так далее), получаемых из компьютерных сетей, а также на съемных носителях информации;

в случае установки или изменения ПО при возникновении подозрения на наличие вирусов проверять на наличие вирусов жесткие диски АРМ, запуская антивирусное ПО для тестирования файлов, памяти и системных областей дисков.

6.6. Сотрудникам запрещается:

открывать приложения и документы в письмах, получаемых по электронной почте, если имеются сомнения в надежности отправителя и (или) отправления;

переходить по ссылкам в спам-письмах;

загружать файлы с сайтов, если имеются сомнения в надежности сайта и (или) загружаемого файла.

6.7. При возникновении подозрения на наличие вирусов сотрудники обязаны:

приостановить все операции, связанные с обработкой файлов на АРМ;

запустить антивирусное ПО для тестирования файлов, памяти и системных областей дисков;

о факте обнаружения вирусов немедленно сообщить системному администратору, владельцам зараженных или поврежденных вирусами файлов, другим пользователям, использующим зараженные файлы в работе;

провести анализ необходимости дальнейшего использования зараженных вирусом файлов;

провести самостоятельно или совместно с системным администратором лечение зараженных файлов, в случае обнаружения не поддающегося лечению вируса удалить инфицированный файл и проверить работоспособность компьютера.

6.18. Сотрудники допускаются к работе на АРМ только после обучения пользованию средствами антивирусного ПО в соответствии с разделом 12 настоящей Политики ИБ.

VII. Криптографическая защита информации

7.1. Криптографическая защита информации (шифрование) применяется для обеспечения конфиденциальности информации при хранении в ненадежных хранилищах и (или) передаче ее по незащищенным каналам связи (телефон, факс, электронная почта и так далее).

7.2. Применение средств криптографической защиты информации (далее - СКЗИ) для шифрования конфиденциальной информации должно осуществляться с учетом требований Приказа Федеральной службы безопасности Российской Федерации от 9 февраля 2005 г. N 66 "Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации".

7.3. Необходимость криптографической защиты информации конфиденциального характера при ее обработке в информационной системе, выбор применяемых СКЗИ устанавливаются в зависимости от класса информационной системы в соответствии с правовым актом города Перми, определяющим порядок эксплуатации информационной системы.

7.4. Шифрование осуществляется перед отправкой данных по незащищенным каналам связи или перед помещением на хранение в ненадежных хранилищах.

VIII. Обезличивание персональных данных

8.1. Обезличивание персональных данных проводится в целях обеспечения защиты от несанкционированного распространения персональных данных при размещении в информационных системах, не предназначенных для обработки персональных данных (далее - открытые информационные системы), и (или) передаче по незащищенным каналам связи.

8.2. Обезличивание персональных данных должно осуществляться с учетом требований и методов, утвержденных Приказом Роскомнадзора от 5 сентября 2013 г. N 996 "Об утверждении требований и методов по обезличиванию персональных данных".

8.3. При использовании процедуры обезличивания не допускается совместное хранение персональных данных и обезличенных данных.

8.4. Обезличивание персональных данных должно производиться перед внесением их в открытую информационную систему и (или) передачей по незащищенным каналам связи.

IX. Регламентация использования электронной почты

9.1. Система электронной почты ЦДТ (далее - электронная почта) используется в информационных целях, в том числе оповещения, организации работы, обеспечения внутренних и внешних коммуникаций.

9.2. Регламентация использования электронной почты осуществляется с целью снижения риска умышленной или неумышленной несанкционированной рассылки информации, заражения информационных ресурсов ЦДТ вирусами.

9.3. Угрозы, связанные с электронной почтой:
возможность создания писем с фальшивыми адресами;
возможность нарушения конфиденциальности электронных писем;
возможность изменения в процессе передачи содержимого электронных писем;
осуществление сетевых атак посредством отправки упакованного в архив сообщения, распаковка которого приводит к выводу системы из строя, заражению вирусами;
получение спама.

9.4. При работе с электронной почтой служащие обязаны:

перед отправкой тщательно проверять сообщения на отсутствие информации, указанной в пункте 9.6 настоящей Политики ИБ;

периодически удалять из электронного почтового ящика ненужные сообщения и перемещать необходимые сообщения в архивные почтовые папки;

проверять сообщения электронной почты на наличие вирусов;

использовать шифрование, обезличивание конфиденциальной информации при ее отправке.

9.6. При работе с электронной почтой сотрудникам запрещено:

отправлять конфиденциальную информацию без предварительного шифрования криптографическим ПО, разрешенным к использованию;

отправлять персональные данные без предварительного обезличивания или шифрования;

отправлять сообщения с иного электронного почтового ящика или от имени другого сотрудника без предоставления полномочий;

использовать электронную почту для создания, отправки, пересылки или хранения любых подрывных, оскорбительных, неэтичных, незаконных материалов, включая оскорбительные комментарии по поводу расы, пола, цвета, инвалидности, возраста, сексуальной ориентации, порнографии, терроризма, религиозных убеждений и верований, политических убеждений, национального происхождения, гиперссылок или других ссылок на веб-сайты, содержащие указанные материалы, массовые рассылки спама;

рассылать компьютерные коды, файлы или ПО, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования, вирусы или другое злонамеренное ПО, программы для осуществления несанкционированного доступа, серийные номера к программным продуктам и программы для их генерации, логины, пароли и прочие средства для получения несанкционированного доступа к платным ресурсам в сети Интернет, ссылки на указанную информацию;

перехватывать, изменять, удалять, сохранять или публиковать сообщения иных сотрудников, кроме случаев, санкционированных руководителями, или в целях администрирования систем;

использовать веб-сервисы Google, Gmail, Hotmail, Yahoo, Яндекс или подобные почтовые системы третьих сторон ("вебмайл") для отправки и (или) получения служебной корреспонденции;

загружать и запускать исполняемые либо иные файлы без предварительной проверки на наличие вирусов установленным антивирусным ПО, переходить по активным ссылкам, полученным от отправителей, если имеются сомнения в надежности отправителя и (или) полученного сообщения.

9.7. Содержимое электронного почтового ящика сотрудника может быть проверено

системным администратором без предварительного уведомления в случае подозрения на осуществление рассылки писем, содержащих вредоносное ПО, спам, информацию, распространение которой запрещено правовыми актами. Информация о выявленных нарушениях направляется руководителю ЦДТ.

X. Регламентация работы в сети Интернет

10.1. Сеть Интернет в администрации города Перми используется сотрудником для получения информации в рамках исполнения должностных обязанностей.

10.2. Регламентация работы в сети Интернет осуществляется с целью снижения риска заражения информационных ресурсов ЦДТ вирусами.

10.3. Доступ к сети Интернет предоставляется сотрудникам с АРМ, закрепленным для исполнения должностных обязанностей.

10.4. Угрозы, связанные с работой в сети Интернет:
легкость перехвата данных и фальсификации IP-адресов в сети Интернет;
заражение вирусами.

10.5. Сотрудникам запрещается:

осуществлять действия, запрещенные законодательством Российской Федерацией;

отправлять конфиденциальную информацию без предварительного шифрования криптографическим ПО, разрешенным к использованию в ЦДТ;

распространять информацию, содержащую подрывные, оскорбительные, неэтичные, незаконные материалы, включая оскорбительные комментарии по поводу расы, пола, цвета, инвалидности, возраста, сексуальной ориентации, порнографии, терроризма, религиозных убеждений и верований, политических убеждений, национального происхождения, гиперссылки или другие ссылки на веб-сайты, содержащие указанные материалы, массовые рассылки спама;

самостоятельно устанавливать на АРМ дополнительное ПО, полученное в сети Интернет;

загружать и запускать исполняемые либо иные файлы без предварительной проверки на наличие вирусов установленным антивирусным ПО;

открывать страницы сайтов, если имеются сомнения в надежности сайта и (или) имеются уведомления о возможном заражении вирусами;

передавать информацию, обрабатываемую в администрации города Перми, посредством иностранных интернет-сервисов, в том числе систем обмена мгновенными сообщениями, голосовой и видеоинформацией (ICQ, QIP, Jabber, Viber, WhatsApp, Skype и другие), социальных сетей (Twitter, Facebook, LiveJournal и другие), облачных сервисов (iCloud, Google Drive, Dropbox и другие).

10.6. Сотрудники обязаны при обнаружении попыток несанкционированного доступа и (или) при подозрении на наличие вируса немедленно прекратить работу в сети Интернет и сообщить системному администратору.

10.7. Вся информация о ресурсах, посещаемых служащим, автоматически протоколируется и при необходимости представляется системными администраторами руководителям.

10.8. Доступ к сети Интернет может быть блокирован системным администратором без предварительного уведомления служащего при возникновении угрозы безопасности информации.

XI. Проведение внутреннего контроля и обучение сотрудников

12.1. В целях выявления угроз безопасности информации, нарушений настоящей Политики ИБ и принятия мер, направленных на предотвращение угроз и нарушений, в ЦДТ осуществляется

внутренний контроль:

12.1.1. обработки персональных данных в соответствии с утвержденными распоряжением администрации города Перми от 24 августа 2012 г. N 81 Правилами осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленными Федеральным законом "О персональных данных", принятыми в соответствии с ним нормативными правовыми актами и локальными актами администрации города Перми.

12.2. Ознакомление служащих с настоящей Политикой ИБ производится при:
приеме на работу;
изменении настоящей Политики ИБ;
обнаружении действий служащих, которые повлекли или могли повлечь нарушение безопасности информации.

12.3. Обучение сотрудников пользованию средствами антивирусного ПО производится при:
приеме на работу;
изменении антивирусного ПО;
заражении АРМ вирусами.

12.4. Ознакомление сотрудников с настоящей Политикой ИБ и обучение пользованию средствами антивирусного ПО осуществляется под подпись в журнале ознакомления (прохождения обучения) с указанием фамилии, имени, отчества служащего и даты ознакомления (прохождения обучения).

XIII. Ответственность за нарушения настоящей Политики ИБ

13.1. Служащие в рамках должностных обязанностей и полномочий несут ответственность в соответствии с действующим законодательством Российской Федерации за:

невыполнение требований настоящей Политики ИБ;

действия или бездействие, ведущие к нарушению информационной безопасности;

действия или бездействие, ведущие к нарушению действующего законодательства Российской Федерации в области информационных технологий.

13.2. При обнаружении нарушения служащими настоящей Политики ИБ системный администратор устанавливает причины возникновения нарушения и направляет служебную записку о выявленном нарушении руководителю функционального (территориального) органа (подразделения) администрации города Перми.

Руководитель функционального (территориального) органа (подразделения) администрации города Перми принимает решение о необходимости привлечения служащего к ответственности.

Системный администратор ведет учет всех выявленных случаев нарушения безопасности информации